



A Hybrid Improved Unequal Secure Cluster Based Distributed Routing Protocol with Quantum Key Distribution to Improve the Performance Measures in Wireless Body Sensor Network

Prakash Muthusamy

Department of Information Technology, Sri Krishna Adithya College of Arts and Science, Coimbatore, India.
drmprakashphd@gmail.com

Senthil Kumar S

Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology, Tiruchirappalli, India.
✉ szenthilkumar@gmail.com

Kanagalakshmi K

Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology, Tiruchirappalli, India.
kkanagalakshmi@gmail.com

Sreejith Vignesh B P

Department of Information Technology, Sri Krishna Adithya College of Arts and Science, Coimbatore, India
authorsree@gmail.com

Received: 23 March 2024 / Revised: 16 June 2024 / Accepted: 02 July 2024 / Published: 31 August 2024

Abstract – A dense network of sensors called the Wireless Sensor Network (WSN) based on ambient circumstances processes, and transmits data to a sink node. Within the entertainment and healthcare sectors, one of the primary areas of development is Wireless Body Sensor Network (WBSN) technology. Because of their limited size, limited cost, limited power consumption, low maintenance requirements, and ease of installation, WBSNs are a desirable option for these kinds of situations. WBSNs offer many advantages, but they also present a number of difficulties character wise, due to their restricted resources viz., finite power supplies, mobility in the network, which include computational power, storage capacity and communication capabilities. Wide range of medical monitoring equipments are available in hospitals but they are not location dependent and mostly difficult to handle due to wired nature of the network. A hybrid Improved Unequal Secure Cluster based Distributed Routing Protocol with Quantum key Distribution (IUSCDRP-QKD) for WSN to correct energy effectiveness while simultaneously boosting reliability and security. A direct and confidential communication between the source and destination is shown, where communication is accomplished by exchanging a single

photon rather than establishing an initial secret key exchange. Quantum cryptography is a quantum mechanics-based mechanism for safeguarding the distribution of symmetric encryption keys. The proposed system key management scheme applying QKD provides security against all the attacks as it uses the quantum key and hence impostors will not be able to predict or catch the secret key, thus providing a robust and unbreakable security to the network. The goal of this work's future directions is to raise the protocol's efficiency percentage to the maximum.

Index Terms – Wireless Body Sensor Network, Quantum key Distribution, Improved Unequal Secure Cluster Based Distributed Routing Protocol, Network Communication, Performance Measures, Quantum cryptography.

1. INTRODUCTION

Due to the wide range of wireless communication, research that is significant has sophisticated and progressed in networks. WSNs, which are comprised of several interconnected nodes, could be deployed within human accessible regions not having the usage of any actual physical

RESEARCH ARTICLE

medium. WSN is a widely recognized emergency system which exists within all main applications. Sensor nodes aid in comprehending and processing of other nodes [1]. The collective goal is achieved in a well-coordinated fashion. The network's lifetime is proportional to the energy consumption in an indirect manner. Due to the reduced energy consumption, the system features a smaller lifetime. A serious threat is a system which is just productive for a small time period. Stereo recuperation, information minimization, and snooze cycle arranging are several techniques for overpowering short lived networks [2].

Regardless of the receptive exploration aspects of WSN at this time there happen to be a top volume of existing issues whereby the networks could be utilized. A number of research areas are monitoring, keeping track of surveillance, creating hands free operation, army uses, and farming. In total instances because of the style of any kind of application, one of the primary goals is keeping the WSN still alive and purposeful [3]. A vital element in this is the manner the system is formed. As a matter of fact, the topology is mainly identified depending on the application program atmosphere and context. The sensor information is generally gathered from the readily available gateways within a certain topology [4]. This particular information will be forwarded to a leader node or even to a starting station referred to as sink. The network size, the energy used, the longevity of the receptors, the data to be perceived and the time, the geography in which the receptors are positioned, the planet, and the context all influence the style and design intricacy of a WSN [5].

WSN is composed and associated with a limited group of sensor systems geographically distributed inside a certain outdoor or indoor setting. A WSN is designed to collect societal details and also the node products' positioning might be noted or even unfamiliar a priori. Community nodes can communicate with all objects, either logically or physically; these consequent actions of social actors a structure focuses on the application [6]. For instance, at this point, a WSN with similar types of architectures could be approaching identical (mesh, star, and so on.). However, maybe this isn't the case for all applications. The logical architecture is essentially determined by the rational function of the connections (tasks, and so on.). It can be haphazard at occasions, or strategy. The approach is chosen based on the availability of system resources [7].

The computational energy capabilities of a system are mostly dependent on a single magnetic generator, centralized methodologies are appropriate. In such instances, this particular unit is liable for management, coordination, and the processing of the sensed information pursuits [8]. Additionally, it forwards this particular information to a sink node as depicted in Figure 1. The primary benefits of the method are as follows:

Centralized systems enable more effective energy managing.

- Roaming is permitted within the system.
- Network coverage examination is made simple.
- Context information accessibility enables a much better program design and style.

WBSNs are used as objective applications for the purpose of monitoring and for the processing of vital health signs and wellbeing, and entertainment of humans [9]. Improving the quality of human life is the primary objective of WBSNs. The following could be used as an example where to maintain the freedom and independence, without having to constantly supervised or be at the presence of a caretaker, the health status of the chronically ill and elderly people can be monitored seamlessly using the technology of WBSN [10]. The major deviations that since the sensor nodes are mostly one to two hops away from purview of a coordinator node [11] and also medium sized to small networks are usually formed with WBSNs is what WBSNs separate themselves from the classical WSNs. With only one hop between the coordinator and the sensor node, the star topology is the most often used topology for these kinds of networks [12]. The group mobility of WBSNs is another important characteristic. WSNs, in contrast to WBSNs, with relatively few mobile nodes are typically static, multi hop networks and medium-to large-scale in size [13].

WSNs and WBSNs use many protocols and standards [14]. The recently release is a specifically designed IEEE 802.15.6 standard for WBSNs in 2013. The IEEE 802.15.4 standard is a more and well-established standard and advanced. Medium Access Control (MAC) and Physical (PHY) layers are the limitation to specify to this standard. Because of its ease of use and widespread adoption, IEEE 802.15.4 is anticipated to continue to be a competitive standard for WSNs and WBSNs [15].

To provide the relevant information to minimize the processing cost and time, WBSN technologies are being step by step developed for utilization in the field of ubiquitous healthcare services to effectively prevent accidents instantly. As shown in Figure 2, with the ambit of interdisciplinary area of WBSN, one could continuously, through the internet with real time updates monitor the health continuously at relatively low cost of expense [16]. To provide an accurate treatment to the patients, it helps by monitoring their history in day-to-day life and their vital signs [17]. E-health is a general expression detailing the use of networks, internet and computers to organize the prescriptions, medical records and the communications in-between experts and medical organizations. A unique characteristic of WBSN system is, it consists of several miniature sensors weighing less, each consisting with one or more physical or physiological sensors. In a topology of a sensor network, these sensors can interact with a network coordinator [18]. In numerous application



RESEARCH ARTICLE

scenarios, WBSN could result in significant mutual communication interference while operating in crowded locations like a hospital. With the aim of reducing the work load and improving hospital staff's efficiency along with the additional improvement of comfort to the patients, and to eliminate medical errors, the use of fault tolerant and high-performance wireless devices utilizing the advancements in wireless technologies is help full [19]. Telemedicine systems

can send data faster by employing multiple networks with protocols for connectivity, data processing and analysis. Using various sensors, WBSN for e-health sensors can be utilized for biometric and medical applications where body monitoring is needed. The above data could help in real time monitoring of the patient's conditions or for further analysis for medical diagnosis by obtaining the sensitive data [20].

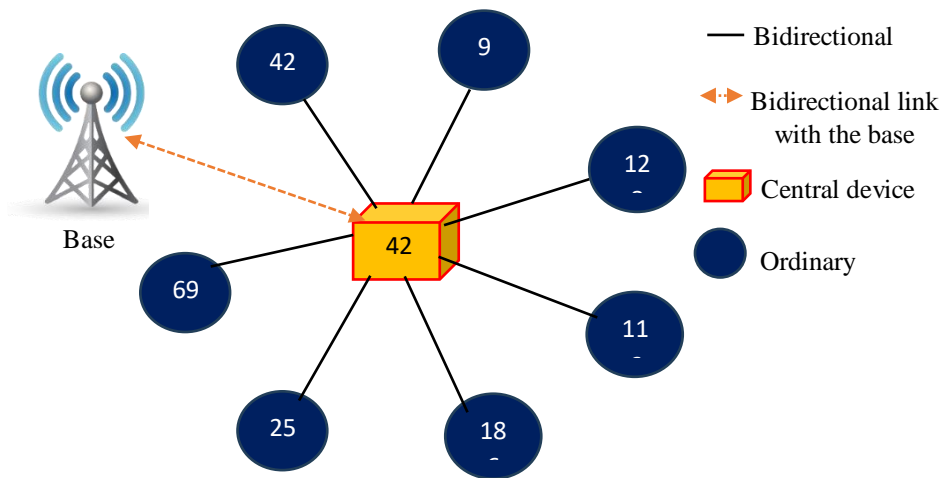


Figure 1 Centralized Strategy

WBANs are self-contained WSN with a specific purpose. It connects a range of therapeutic sensors and devices that are placed both within and outside the human body. It forms a remote monitoring and data collection system from a patient's body. WBANs entail remote access to very crucial and sensitive data, they demand exceedingly high level of privacy and security while processing and storage [21]. As a result, a range of security features that guarantee data protection, privacy, integrity, and confidentiality should always be present in the implemented WBAN architecture. Nowadays sensors are available for monitoring heart rate, pulse rate, blood pressure and glucose levels, allergic agent levels, the quantity of nitric oxide released from suspicious cells, etc. These sensors are usually wearable and are used to measure parameters in the human body. Cardiovascular illnesses can also be treated with WBANs [22].

The Network layer is accountable of routing. For numerous WBANs, routing is done using sink nodes. Spoofing, wormhole, sinkhole, selective forwarding, Sybil, and hello flood attacks are all possible in this layer. Spoofing occurs when an enemy node generates bogus error signals [23]. Selective forwarding is an attack where an attacker dumps packets anywhere in the network and then by choosing it passes them to neighbour nodes. A sinkhole attack occurs when a rogue node draws all data packets in the network, preventing them from reaching their intended destination. A wormhole threat arises when an enemy node captures all

packets in one location prior to actually tunnelling them to another [24]. This exploit can occur even in the early stages of the network, when nodes begin to identify packets from neighboring nodes. When one node exhibits itself to have several identities in a network, it is called a Sybil assault. HELLO flood attack occurs when an attacker posts a HELLO packet to the network with a strong radio signal to dupe other nodes in the network that they should route traffic via them [25].

The Wireless Multimedia Sensor Network (WMSN) is a system of wirelessly linked sensor nodes with multimedia products as digital cameras and microphones that may access videos and also sound channels, nevertheless pictures, along with scalar sensor information [26]. Surveillance sensor networks, police accounts, traffic managing methods, sophisticated healthcare shipping and delivery, automatic assistance to senior's telemedicine along a manufacturing course of action management are just some of the likely applications for WMSNs within equally military and civilian ways. Figure 3 illustrates the general performing of MWSN [27].

The Cluster Head (CH) is responsible for cluster relay network, and edge devices, which are divided into various hubs with particular project abundances, according to the overall quality criterion, along with the retention of energy, accumulation of data, stability, extensibility, and so on. A



RESEARCH ARTICLE

much better outcome compared to the previous variation is created by this method. Within the procedure of preserving energy, WSN must get rid of the unwanted node and supply fused information to several hop nodes that continue to be effectual terminology. With sensor nodes routing table is set

up to be able to minimize the dimensions of the information clustering. A lesser amount of energy use is accomplished by intra and inter clustering methods. Latency is attained by a collision management mechanism [28].

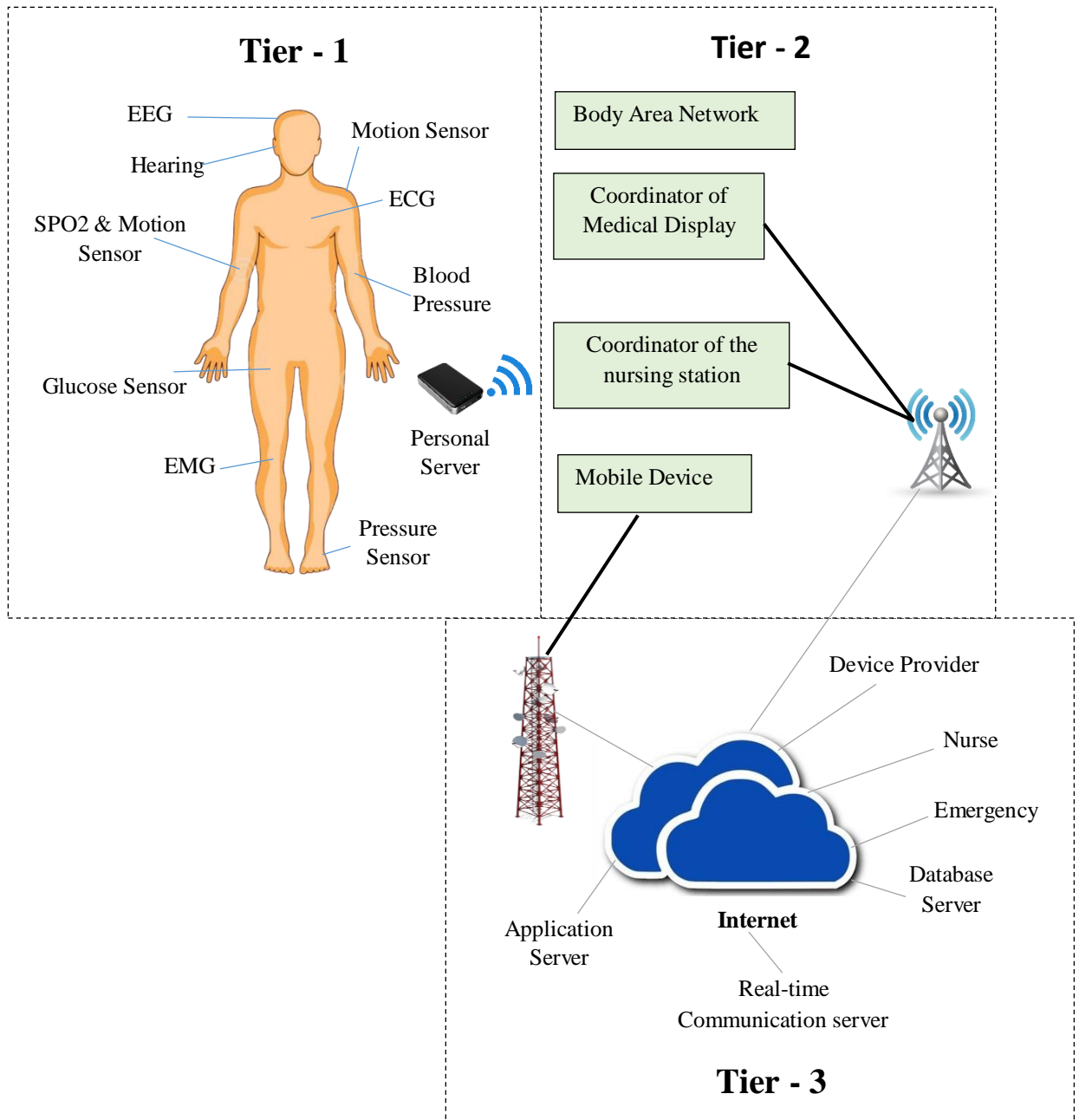


Figure 2 System Diagram of WBSN in Telemedicine

RESEARCH ARTICLE

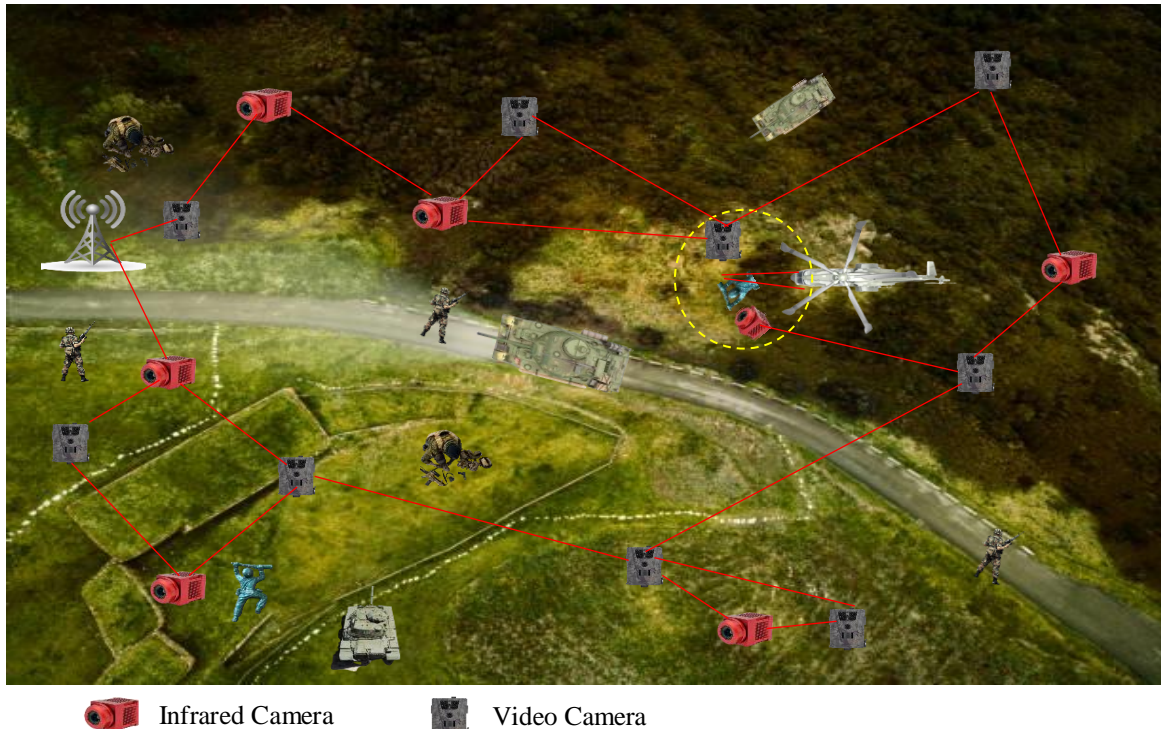


Figure 3 Multimedia WSNs

1.1. Research Motivation

In general, WSN in healthcare has the responsibility to deliver all the sensed packets to the destination. The packet loss in WSN is considered as an inevitable factor that occurs due to various network characteristics, such as low Received Signal Strength Indicator (RSSI) and distance high interference and quantity of devices. The packet loss prevention is addressed by various WSN techniques such as, centralized, hierarchical and static. But these techniques require more resource sharing for data collection and processing. The chief lacuna of present healthcare systems is the use of wired/fixed systems and their associated wired biomedical sensors. They are additional constrained by patient's mobility, size, transmission capacity and power. One should keep the sampling rate and power consumption at minimal level, for expanding the current health care systems to Mobile Health (MH), Electronic Health (EH), Internet Health (IH) and Ambulatory Health Monitoring Systems (AHMSs). There is a critical need to minimize hospitalization time and costs for the next generation. This is our main motivation for providing new wireless healthcare systems. The need of the hour, in the current healthcare system, the medical experts should be provided with further adaptations for monitoring wirelessly several patients at a time by improving signal integration and visualization, and extended mobility. The amount of data increases rapidly in the healthcare system since monitoring takes place over an extended period of time. Therefore, to provide Wireless

Healthcare Systems (WHSs), it is crucial to lower a load of sampling by combining the sampling and compression phases. This would decrease the utilization of storage, transmission delays, and power consumption. By eliminating time and location constraints of a patient; anytime and anywhere the doctors and physicians could be provided vital information of a patient's body by the WHSs which would improve the quality and mobility of healthcare system.

1.2. Problem Statements

The sensor nodes have limited resources. The sensor nodes are placed in a potentially hazardous area. This phenomenon, known as the "hot-spot problem," occurs when nodes that are closest to the sink tend to use up their energy more quickly than other nodes. In a WSN, many data transmissions lead to congestion at the nodes close to the base station. Congestion control should be precise and rapid to avoid any loss. Congestion in WSNs raises data breach rates and data communication energy usage. Congestion lowers the WSN's routing performance and causes data loss during transmission. Congestion in WSN is a important issue that needs to be fixed.

1. Use of mobile node to achieve the balanced energy consumption, the congestion control, and the balancing rate.
2. To design Power Efficient (PE) and High Throughput (HT) Multi-Hop Routing Protocol for WBSN.

RESEARCH ARTICLE

1.3. Objectives

1. To provide a safe and efficient system for enhancing WBAN security and authentication.
2. To provide an Integrated Security paradigm facilitating secure communication in WBANs with limited resources.
3. To build an efficient key management strategy that provides unbreakable security.

Organization of the paper as follows: Section 2 describes the related work of WSN in all routing protocols, WBSN in healthcare and Data transmission using network. Section 3 describes the proposed work in detail and the case study of where the proposed system applied. Section 4 discusses the experimental results based on network lifetime, throughput, and energy consumption comparison of proposed and existing systems. And section 5 concludes it.

2. RELATED WORK

Latest advances in electronics and wireless network systems have leapfrogged the development of medical sensors which are intelligent and small and some actuators which could be planted in the human body or wearable. Patient's physiological parameters are researched and transmitted to medical center in a more reliable and efficient way. WSNs are an upcoming technology that can be used remotely to monitor a variety of medical situations at a minimal cost [29].

Obligations to the latest developments of hardware production engineering and cost-efficient software program algorithms, the deployment of a system composed by thousands or hundreds of little, inexpensive wireless receptors has these days turned out to be attainable. These sensor nodes are resource constrained products, effective at carrying out small calculations, computing details and talking with neighbouring devices [30]. Being a WSN will normally consists of a significant quantity of nodes, the gadgets need to be inexpensive and small; in addition, as a way to maximize the system lifetime have to guarantee a reduced energy usage [31].

A number of uses were recommended for WSNs, which range from environmentally friendly keeping track of army uses, against healthcare hygiene on the control of home electric products, and so on. Thus, a number of different specifications emerge, with respect to the particular program and on the context in which the system needs to be deployed. Nevertheless, since interaction is easily the highest priced practice of terminology of electrical energy usage for a sensor node one common objective for WSN applications is reducing that much the quantity of information to become transmitted as practical. This information usually includes sensor readings which must be gathered up and transmitted towards the gathering thing by way of multichip reception [32].

For WSN, the style and design job of routing protocols is fairly demanding because of a number of attributes that differentiate them against wireless infrastructure with less networks. Inside WSNs, various kinds of routing conflicts can be found exactly where several of them are talked about below. It is around intricate to designate a common identifiers process for sensor nodes with top amount. As a result, wireless sensor nodes aren't effective at making use of protocols based upon classical IP. The information that is recognized is important coming from various energy sources to a specific foundation station. Nevertheless, that doesn't take place in regular correspondence networks [33].

In the majority of instances, the information that is produced has crucial redundancy as numerous realizing nodes are able to make very similar details while detecting. Thus, it is essential wear these redundancy from the routing protocols, the accessible bandwidth and vitality [34]. Since the sensor nodes are battery powered, a restricted level of energy. Throughout information transmission, a tremendous volume of electrical energy is consumed. Furthermore, the path finds and upkeep phases may take a huge amount of energy. The network's lifetime is specifically proportional on the complete energy ingested by every node. Whenever a sensor node's energy goes down under a particular threshold, it gets non-functional and contains an influence on the network's efficiency [35].

Most sensor nodes inside an aimed diffusion-based community are application aware, and that allows obtaining energy cost savings by choosing empirically excellent paths by diffusion and also by caching and processing details within the system. Caching is able to up the effectiveness, scalability and robustness of control between sensor nodes that is the heart of the information diffusion paradigm [36]. Additional use of directed diffusion is usually to spontaneously propagate a crucial occasion for some areas on the sensor system. This kind of information retrieval is nicely suited just for chronic queries exactly were asking for nodes aren't wanting information which gratify a query for period of time. It is then unsuitable for one-time queries, as it is not well worth establishing gradients for queries, and utilize the road only one time [37].

In AODV routing protocol, only when the source has data to send does the destination's route become apparent. Initially, checking its own routing table, the node, if there exists a route, it transmits the data. It broadcasts a RREQ packet to find the destination's route in the event of unavailability of information. When RREQ packet is received by any node, its own routing table is also checked. On the availability of the route, the node sends RREP to reach the destination with the path as reply. This reply packet follows the same path which is followed by the request packet. The node rebroadcasts the route request packet if the routing table contains no path. On

RESEARCH ARTICLE

discovery of the destination source through the path, all the packets are forwarded by the same route. If the source node does not get any reply till the timer expires, the request packet is again rebroadcasted. The AODV protocol's primary flaw is the requirement for numerous packet transfers. A single request packet generates numerous multiple reply packets in response. When a path is discovered, all the packets are transferred by the same route. The energy consumption of the network is unbalanced as a result of the nodes along the path losing energy [38].

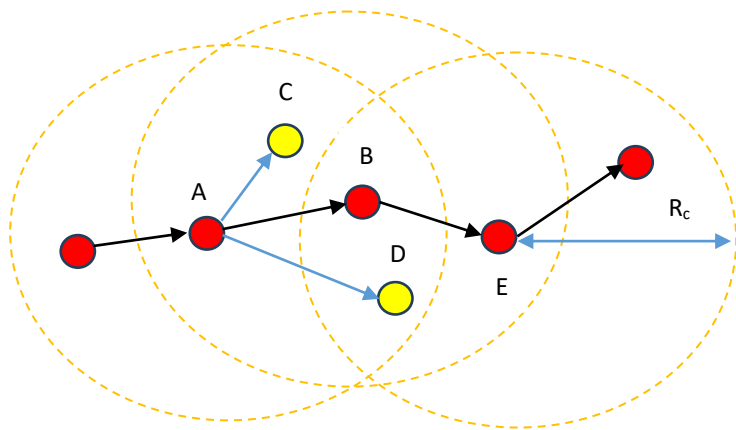


Figure 4 Data Transmission in WSN

The sensor nodes calculate their location (x, z). The node whose timer expires first broadcasts the header advertisement message within its own grid. The node with the lowest identifier wins and becomes the header if two distinct nodes transmit advertisements simultaneously. The header's actual position is known to the cluster's nodes. So when the data comes in neighbour cluster region, it is forwarded to the header. In this way, data is transferred towards representative header to access node [39].

As shown in Figure 4, the node S is source node and R is the receiver node. The intended path is S-A-B-E-R from source to destination. Node C is in communication range of node A and node B whereas the node D is in communication range of A, B, and E also. The node A is multicasting the packets. When node B does not receive the packet from node A, the node C will act as the cooperative node. Node C also has the copy of the data packet sent by node A which it will forward to node B. The node is the sender's co-operator node. Similarly, Node D can also act as the cooperative node because it is a range of node A and E. So the node D can be said as receiver's co-operator node [40].

When patient-related data is accessed through local servers and the Internet, privacy and security are two major concerns that must be addressed in WBAN; there is a need to develop a safe system in WBAN [41]. It has been observed that medical datasets pertaining to numerous ailments are available via the

Internet and are readily accessible to everyone. There is a challenge in that, the patient's profile, and his or her medical information, must be safeguarded using any conventional mechanism. It's also critical to use sensors in any urgent situation to collect and process patient data to retain security and eco-friendly conditions. When saving and retrieving patient-related data, there is always the dilemma of how to assure security [42].

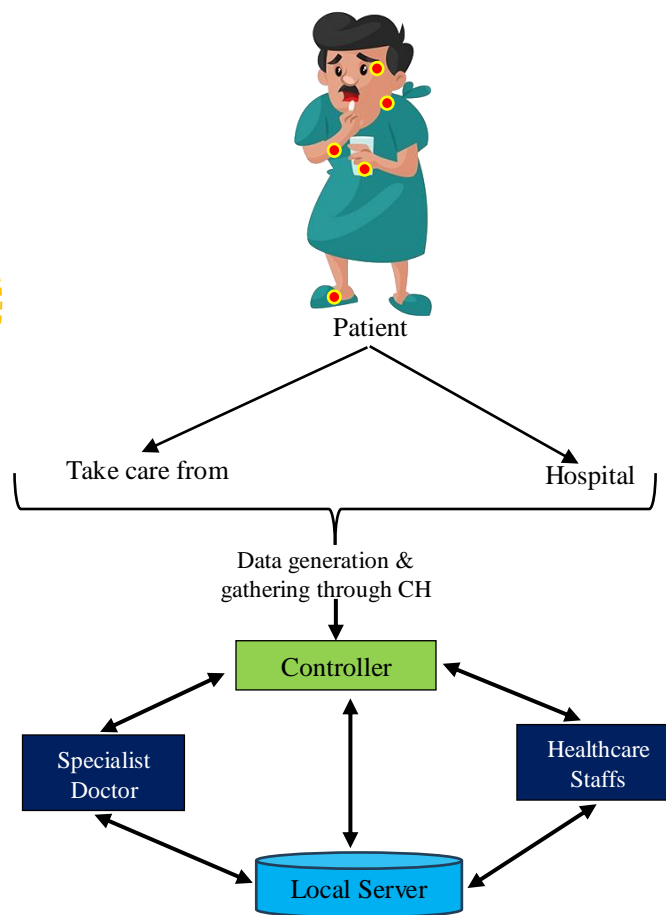


Figure 5 WBAN – Three Tier Architecture

WBAN works in any context where a variety of personnel have access to the data, such as healthcare workers, doctors, nurses, lab technicians, and so on, and where attackers have easy access to the data. Cyber-attacks on these types of networks, such as attempts to manipulate progressive metering mechanisms, have formed to be a real threat. We describe our preliminary findings in this study, which include an investigation of the body sensor network using Routing for Low-Power and Lossy networks (RPL) under packet drop attacks, which could be launched by advance calibrated jammers and have a negative influence on such Body Sensor Networks. Figure 5 depicts WBAN's three-tier architecture, with tier 1 being responsible for sensitive data collection and

RESEARCH ARTICLE

storage, layer 2 for data processing between Sensor nodes and Cluster Heads, and tier 3 for data processing between Cluster Heads - CHs and Controller Nodes - CNs. Figure 5 depicts the several sensors that have been implanted in a patient.

The Controller Node - CN is in charge of disseminating critical information without jeopardizing authentication and security. This three-tier design implies that a patient's body has various sensors that must be sent to controller node CN without jeopardizing security. As a result, certain sensor nodes are configured to operate as a CH to ease communication while also providing security and authentication. The secret key creation and management process is divided into three tiers, with the first tier involving key generation between sensor node N and CH, the second tier involving key generation between CH and CN, and the third tier involving key generation between CN and CH [43]. When an attacker performs the steps listed above, the targeted router is unable to relay any packets to its parent node. An externally induced black hole attack can be created because the attacker can discard all packets over the targeted network forever without having to damage the internal logic of a legitimate router.

Since several WSN offer self-organizing, self-configuring, self-diagnosing, and then self-healing abilities on the sensor nodes, allow for speedier deployment and setting up of different kinds of sensor nodes. Additionally, it offers connectivity mobility and convenience, enabling community development as-needed. Information is transferred via intermediate sensor nodes inside a wireless sensor system that is a multi-hop network. The contacts in between sensor nodes are incredibly susceptible to disappointment. The frequency of link malfunction includes an immediate effect on the information shipping and delivery ratio and also the network's dependability [44]. This issue motivates the improvement of reliable routing strategies. Consequently, the aim of the analysis is using WSN to exchange non compatible wired community methods. Additionally, advanced microcontrollers with energy consumption that is low could be utilized to produce sensible WSN nodes.

3. PROPOSED METHOD

WSN is a system of wirelessly interconnected products which are distributed with a part of fascination. The constituting aspects of a WSN are definitely the sensor nodes and a minimum of one sink node, known as the starting station. A common sensor node is a Micro Electromechanical Structure (MEMS) which, in spite of its constrained materials within terminology of computation, communication, memory, and energy, is in a position to do realizing, information processing. A starting station is unit full of energy, computational, correspondence materials which records the information transmitted to itself, through the sensor nodes, and functions being a supervisory controller on the WSN, an

entry thing for man user interface, along with a gateway to various other networks. A WSN, based mostly along the combinational utilization of the sensor nodes of its and the base station(s) of its, is in a position to keep track of the background problems more than broad areas of fascination and deliver information that is relevant to distant destinations. This is the reason WSNs are regarded as to become the Centre of Internet of Everything (IoE) and help support a constantly changing variety of man tasks associated with industry, agriculture, reconnaissance and surveillance, sensible houses, sensible towns, planet and habitat keeping track of, biomedical uses, army uses automobile traffic management, flame detection, listing management, farming, printer disaster analysis, along with energy managing applications as proposed shown in Figure 6.

The three main phases of the proposed IUSCDRP-QKD are cluster maintenance, secure information transfer, and uneven cluster development. Figure 6 provides an illustration of the general process. Following the deployment of the nodes inside the WSN, BS sends an initialization packet to every single node within the WSN. When a Received Signal Toughness Signal (RSSI) is used, each node's distance to the Base Station (BS) is measured, and this information is useful for assembling uneven measurement clusters.

The integration of MEMS (Micro-Electro-Mechanical Systems) sensors is crucial. Here, we provide specifics on the types, data acquisition rates, sensitivity, and integration of MEMS sensors in such a system:

Accelerometers and Gyroscopes: Measure acceleration forces and are used for monitoring body movements. Typically operate at data acquisition rates ranging from 50 Hz to 1000 Hz, depending on the precision required and the specific application. For body movement monitoring, rates around 100 Hz are common. Sensitivity is often in the range of $\pm 2g$ to $\pm 16g$, with resolutions from 1 mg to 5 mg and Gyroscopes range from $\pm 250^\circ/s$ to $\pm 2000^\circ/s$ with resolutions around $0.01^\circ/s$.

Pressure Sensors: Measure blood pressure or other pressure-related metrics. The data acquisition rate can vary but typically ranges from 10 Hz to 100 Hz for real-time monitoring. Sensitivity can be as precise as ± 1 mmHg, crucial for accurate blood pressure monitoring.

Temperature Sensors: Monitor body temperature. These sensors usually have lower data acquisition rates, around 1 Hz to 10 Hz, as body temperature changes slowly. Sensitivity usually around $\pm 0.1^\circ C$.

Heart Rate Sensors: Measure the heart rate and other cardiovascular metrics. Often have acquisition rates around 100 Hz to capture detailed cardiovascular waveforms. Sensitivity typically allows for detection of variations of less than 1 beat per minute (BPM).

RESEARCH ARTICLE

Electromyography (EMG) Sensors: Measure muscle electrical activity. Require higher data acquisition rates, typically between 500 Hz and 2000 Hz, to accurately capture muscle activity. High sensitivity required to detect microvolt-level signals from muscle fibers.

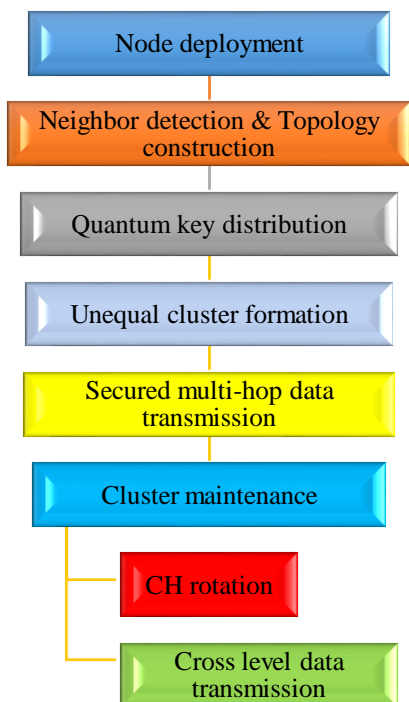


Figure 6 Block Diagram of IUSCDRP- QKD

3.1. Integration of MEMS Sensors

Cluster-Based Architecture: MEMS sensors are organized into clusters based on the body area or type of monitoring. Each cluster communicates with a central node (often a smartphone or a dedicated health monitoring device).

Data Fusion: Integrating data from multiple MEMS sensors to provide comprehensive monitoring. For example, combining accelerometer and gyroscope data for accurate motion analysis.

Energy Efficiency: Given the limited battery life of wearable devices, MEMS sensors must be energy-efficient. This is achieved through duty cycling (turning sensors off when not needed) and efficient communication protocols.

Secure Communication: Quantum Key Distribution (QKD) ensures secure data transmission between sensors and the central node. This is crucial for protecting sensitive health data.

Processing and Storage: Data from MEMS sensors are often pre-processed locally (e.g., noise reduction, signal filtering) before transmission. The central node performs more extensive processing and stores the data.

Real-Time Monitoring: The integration must support real-time data acquisition and analysis to provide timely feedback and alerts. This is critical for applications like heart rate monitoring, where immediate response can be life-saving.

Data from these sensors are collected by a central node (e.g., a wearable hub or smartphone) which uses QKD for secure data transmission. The system uses an improved unequal secure cluster-based distributed routing protocol to manage data transmission efficiently, balancing energy consumption across the network and ensuring reliable data delivery. By integrating these MEMS sensors with advanced routing protocols and QKD, the performance of Wireless Body Sensor Networks can be significantly enhanced, providing accurate, real-time health monitoring while ensuring data security and network efficiency.

3.2. Initialization of Packet Structure

The initialization packet is critical for setting up the network and establishing communication parameters between nodes. Table 1 shows the structure of an initialization packet in a WBSN using the hybrid improved unequal secure cluster-based distributed routing protocol with QKD:

Table 1 Initialization of Packet Structure

Field Name	Size (bits)	Description
Packet Type	8	Indicates the type of packet (e.g., Initialization = 01)
Source ID	16	Unique identifier of the source node
Destination ID	16	Unique identifier of the destination node (e.g., Sink ID)
Cluster ID	8	Identifier for the cluster to which the node belongs
Node Role	8	Specifies the role (e.g., Cluster Head = 01, Member = 02)
QKD Key Info	128	Quantum key information for secure communication
Timestamp	32	Time at which the packet is sent
Energy Level	8	Current energy level of the node (0-255 scale)
Location Info	64	Geographical or relative location information

RESEARCH ARTICLE

Sensor Type	16	Type of sensor (e.g., Accelerometer = 01, Temperature = 02)
Data Acquisition Rate	16	Sampling rate of the sensor (in Hz)
Reserved	32	Reserved for future use
Checksum	16	Error-checking field for packet integrity

This structured approach to deployment and initialization ensures efficient, secure, and reliable operation of the WBSN, enhancing its performance in monitoring and managing health data. Clustering inside WSN partitions the nodes in clusters, by way of a selected CH for every cluster, and also the rest of the nodes are called as cluster participants. The procedure for CHs choice exclusively is determined by the rest of the energy amount. The cluster development of WSN is

illustrated with Figure 7. At first, a lot of prospect CHs are decided to participate for ultimate CHs. Each node turns into an applicant CH together with the same likelihood T which happens to be a fixed threshold. Plus, the rest of the nodes become rest suggest till the CH buying process terminates. Consider allowing n_x to be an applicant for CH together with the competitor's radius R_{com} . The goal is to ensure that, should n_x be chosen as the CH, no other CHs n_x take place within a comparable competitor's range. The sectors indicate a number of R_{com} of prospect CHs inside their topology in Equation (1).

$$n_x \cdot R_{com} = \left(1 - k \frac{d_{max} - d(n_x, BS)}{d_{max} - d_{min}}\right) R_{comp}^0 \quad (1)$$

Wherever d_{max} - maximum distance; d_{min} - minimum distance; and k - frequent coefficient together with the values in between zero and one. Making use of the Equation (1), the R_{com} differs within the assortment of (1-c) R_{comp}^0 to R_{comp}^0 .

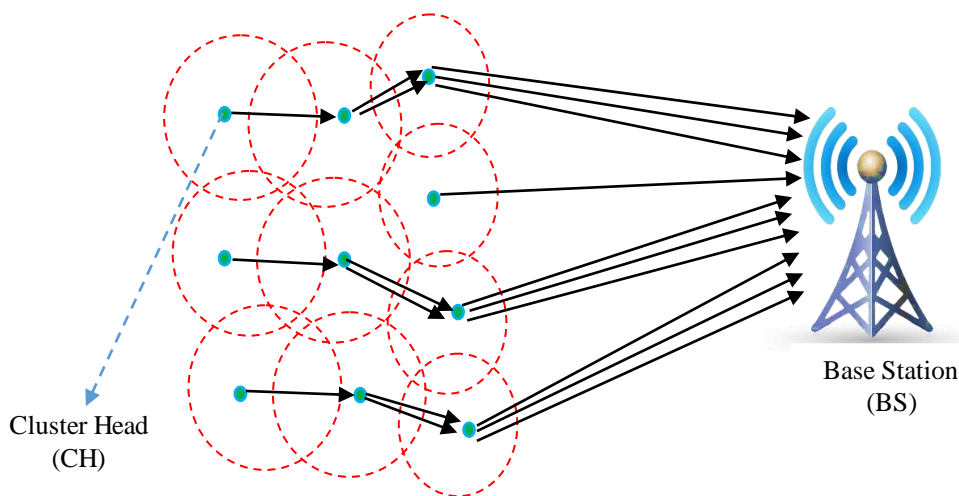


Figure 7 Cluster Formation in WSN

3.3. Cluster Head Selection Algorithm

Step 1: Initialization

Each sensor node initializes itself with a unique identifier and an initial energy level.

Step 2: Threshold Calculation

Each node calculates a threshold value ($T(n)$) based on a predetermined percentage of remaining energy ($P(n)$). The threshold is a random value between 0 and 1. If $T(n) < P(n)$, the node becomes a candidate for becoming a CH for the current round.

Step 3: Cluster Formation

Nodes compare their threshold values with the calculated threshold. If a node's threshold value is lower than its

remaining energy percentage, it becomes a candidate CH for the current round.

Nodes that choose to become CHs broadcast an advertisement message to all nodes in their vicinity, declaring their candidacy.

Step 4: Cluster Setup:

Nodes not selected as CHs join the cluster of the nearest CH based on signal strength or proximity.

Each CH collects information about the nodes that have joined its cluster.

Step 5: CH Rotation

RESEARCH ARTICLE

To distribute energy consumption evenly across the network and prevent premature energy depletion of CHs, CHs may rotate periodically.

The rotation schedule may be based on factors such as the number of rounds elapsed or the total number of CHs in the network.

3.4. Parameters

- Node Energy Level (E): Initial energy level of each sensor node.
- Threshold Value (T): Random threshold value calculated by each node based on its remaining energy percentage.
- Percentage of Remaining Energy (P): Predetermined percentage of remaining energy below which a node decides to become a CH.
- Round Number: Current round of CH selection.
- Transmission Range: Maximum distance over which a CH can communicate with nodes in its cluster.

The CH selection algorithm in hierarchical clustering-based protocols like LEACH ensures efficient utilization of energy resources by evenly distributing energy-intensive tasks among sensor nodes. By dynamically selecting CHs based on thresholds and periodically rotating CHs, the algorithm enhances network longevity and stability in wireless sensor networks.

3.5. Secure Strategy to Transmit Data

The dynamics of hands-on process, all of the routes are approximated previously towards the necessity inside the proposed IUSCDRP-QKD method. While the sensor nodes are being fixed, it seems more tempting to use a table-driven protocol rather than using a reactive approach.

Initially, during the deployment phase, every node is carrying a certification, a distinct ID, a public key, and a unique shared element. A unique shared key element is used to communicate with BS, and the certification is used for authenticity throughout the system lifespan when identifying a neighbour using the BS public element.

The secured transmission of IUSCDRP-QKD consists of four phases, which include neighbour detection, quantum critical division, re-routing, and spoken data delivery in addition to topology creation.

3.6. Topology Construction and Neighbour Detection

Every node has a unique shared major (Kxbx), public key (Puk), certificate (CERTx), and ID (IDX) computed using Equation (2).

$$i \rightarrow *: NBR_DET | ID_i | CERT_i \quad (2)$$

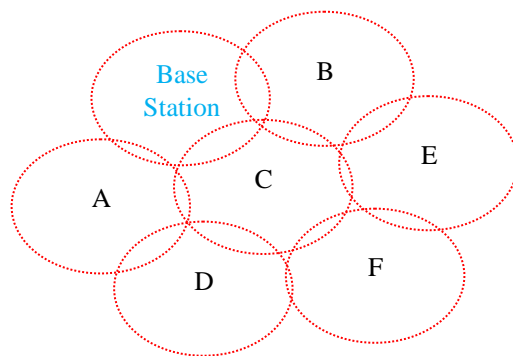


Figure 8 Detection of Neighbour

The node next pushes the ID to neighbor_list, on authentication of sender node or maybe it casts off the package. Thus, the illegal node doesn't take part in the stage of neighbour detection shown in Figure 8. It starts to send the neighbour's information on the BS as soon as the transmitted using Equations (3) and (4):

$$i \rightarrow BS: NBR_INFO | ID_i | CERT_i | (k_{ibs}, NBT_i) | \quad (3)$$

$$MAC(k_{ibs}, NBS_INFO | ID_i | CERT_i | E(k_{ibs}, NBR_i) | \quad (4)$$

The next activities are performed all intermediate nodes which get the NBR_INFO packet: The authenticity is validated mainly through certification. When generally the availability of authenticity found sender node is affirmed, the nodes in the receiver resend the package.

It reduces the system visitors within this particular fashion and also economizes the node power. MAC is utilized that's created by the information and encrypted through the distinctive shared element, within such a fashion which nobody may adjust or maybe spoof the neighbour information shown in Figure 9.

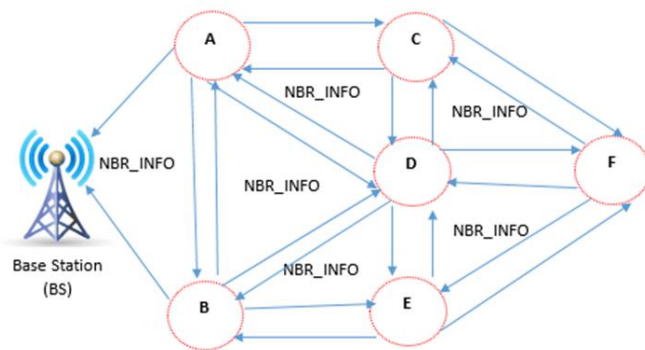


Figure 9 Broadcasting in WSN

Each node initializes itself and starts broadcasting beacon messages to discover neighboring nodes. Nodes listen for beacon messages from neighboring nodes within their communication range. Upon receiving beacon messages, nodes identify neighboring nodes based on signal strength or

RESEARCH ARTICLE

proximity. Nodes use asymmetric cryptographic algorithms like RSA or ECC to authenticate neighboring nodes. Digital signatures are exchanged to ensure the authenticity of beacon messages.

3.7. Quantum Key Distribution

The BS ideal community topology and also generates an adjacent matrix right afterwards getting the neighbour information by almost all the nodes within the system consequently. For every neighbour node pair, a starting station needs to calculate secret element which is viewed as quantum key element using Equations (5) – (7).

$$k_{ij} = h(secret, ID_i, ID_j) \quad (5)$$

$$BS \rightarrow i: \text{QUAN_KEY} | \llbracket seq \rrbracket_no | \llbracket ID \rrbracket_bs | \llbracket CERT \rrbracket_bs | \llbracket ID \rrbracket_i | \llbracket ID \rrbracket_j | E(k_{ibs}, k_{ij} | E(k_{jbs}, k_{is})) \quad (6)$$

$$MAC(k_{ibs}, \text{QUAN_KEY} | \llbracket seq \rrbracket_no | \llbracket ID \rrbracket_bs | \llbracket CERT \rrbracket_bs | \llbracket ID \rrbracket_i | \llbracket ID \rrbracket_j | E(k_{ibs}, k_{ij} | E(k_{jbs}, k_{is})) \quad (7)$$

- The structure of an ID is comprised of a packet, neighbor ID, destination ID, sequence_no, packet_type, certificate, MAC and encrypted quantum key for y and x. Each and every intermediate node acquiring the package works.
- The BS certification validations occurs with the public element.
- It retailers the node pair, sequence_no, kind of package and retransmits the package when generally there is available absolutely no entry within that particular kind or maybe it drops using Equations (8) – (9).

$$i \rightarrow j: \text{CHALLENGE} | ID_j | (k_{jbs}, k_{ij} | E(k_{ij}, ID_i | nonce)) \quad (8)$$

$$j \rightarrow i: \text{CHALLENGE_REP} | ID_i | (k_{ij}, ID_j | nonce + 1) \quad (9)$$

The neighbouring nodes could verify one another within this fashion by task package swapping along with repetitively mailing the related pair wise key to y were definitely reduced. Each and every pair on the node has a quantum element during the ultimate stage. Within the preferred structure, when x doesn't gain CHALLENGE_REP package, it could transmit an article to BS over phony node which has ID and certificate of respectable node using Equations (10) – (13).

$$i \rightarrow CH: \text{DATA} | ID_i | (k_{ich}, d_i) \quad (10)$$

$$MAC(k_{ich}, \text{DATA} | ID_i | E(k_{ich}, d_i)) \quad (11)$$

$$CH \rightarrow BS: \text{AGGR_DATA} | \llbracket ID \rrbracket_ch | \llbracket ID \rrbracket_j | (k_{ich}, \llbracket seq \rrbracket_no) | E(k_{chbs}, d_{ch}) \quad (12)$$

$$MAC(k_{chbs}, \text{AGGR_DATA} | seq_{no} | E(k_{chbs}, d_{ch})) \quad (13)$$

After transforming the Data to bits of 0s and 1s and then sent using polarized photons in quantum cryptography. The recipient observes the photons that the sender has placed in a

particular quantum state. There are four possible polarizations for a photon: 90, 0, 45, or -45 degrees, and is measurable in three ways: rectilinear (horizontal or vertical), circular (left-circular or right-circular), or diagonal. In this case, just the rectilinear and circular bases are used. The receiver can discriminate between polarizations of 0 and 90 degrees, or -45 and 45 degrees. Any measurement of photon alters it and therefore, due to physical considerations, it is not possible to do both observations.

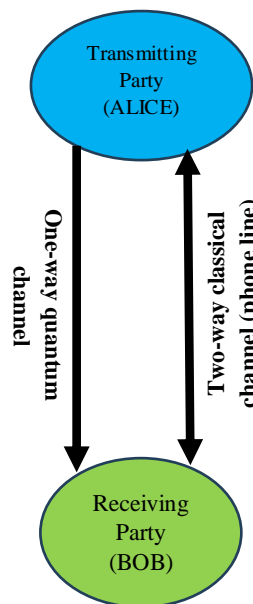


Figure 10 Communication Channels Involved in IUSCDRP-QKD

Therefore, in addition to receiving the signals, the receiver needs to measure them in relation to the appropriate bases. This information could not be sent in between the transmitter and the recipient for the reason it would allow a third party to access the secret key if it was intercepted. Instead, the receiver selects one of the two polarizations at random: either 0 and 90 degrees, or -45 and 45 degrees, for each signal. The recipient then calls the transmitter and discusses which form of measurement is used for each bit in public. The transmitter verifies which bits are valid, and both the transmitter and recipient discard any bits that were not precisely measured. This forms the key. Furthermore, when sending and receiving parties compare their groups of bits in this way and if they decide to remove a mutually agreed bit, such as the final one, the parity disclosed becomes meaningless to any eavesdroppers. Two channels are used to communicate between two parties: a two-way classical channel and a one-way quantum channel as illustrated in Figure 10. IUSCDRP-QKD is a key generation mechanism that employs quantum mechanics to generate symmetric keys using these two rules, the Heisenberg Uncertainty Principle and Quantum Entanglement.

RESEARCH ARTICLE

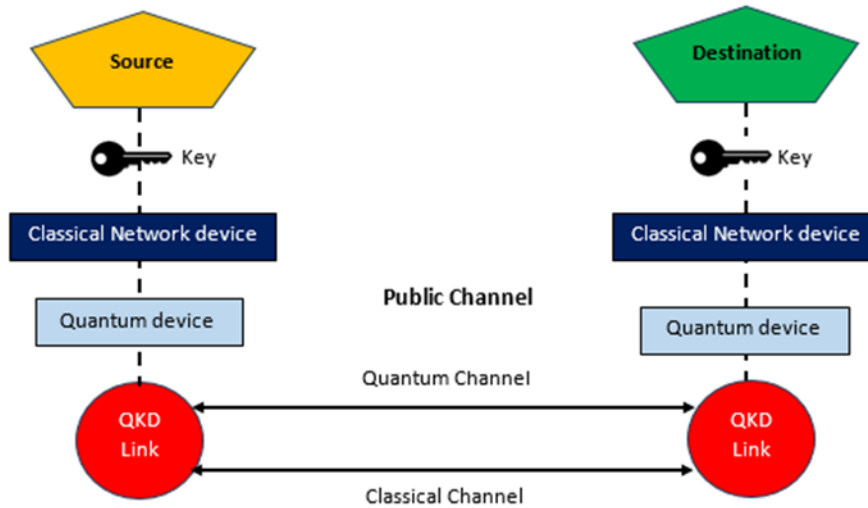


Figure 11 Conceptual Framework of Implementing IUSCDRP-QKD in WBAN

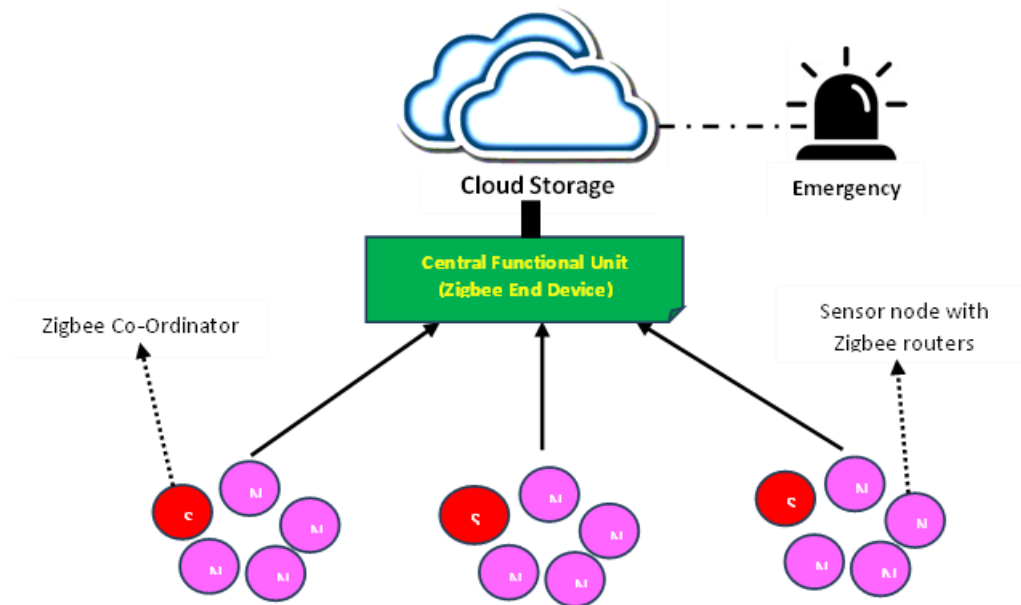


Figure 12 Required System Architecture of IEEE 802.15.6

The various steps formulated in implementing this security mechanism is illustrated in Figure 11. Initially we generate a random WBAN network and we build a random clustered architecture. Clustering of the nodes helps us to overcome the node constraints and network load. The communication between the sensor nodes is enabled using Zigbee technology, a global standard developed to address the needs of wireless IoT networks. Thus, we syndicate the IEEE 802.15.6 WBAN network to operate with IEEE 802.15.4 Zigbee technology and the security framework to the network is implemented using the BB92 IUSCDRP-QKD protocol enhanced with a bitwise operator. This ensures the source and destination

nodes generate the secure key using the polarized photons making it impossible for the intruders to hack the secret key shown in Figure 12.

QKD relies on the principles of quantum mechanics to establish secure communication channels, leveraging quantum states such as photon polarization or spin states for transmitting cryptographic keys. These keys are used to encrypt and decrypt data exchanged between nodes, ensuring confidentiality and integrity of the transmitted information. QKD protocols utilize dedicated quantum channels for transmitting quantum states between nodes. These channels can be implemented using various physical mediums such as



RESEARCH ARTICLE

optical fibers or free-space optical links. Optical fibers offer low loss and high transmission fidelity, making them suitable for short to medium-range communication, while free-space

optical links enable long-distance communication without the need for fiber-optic cables.

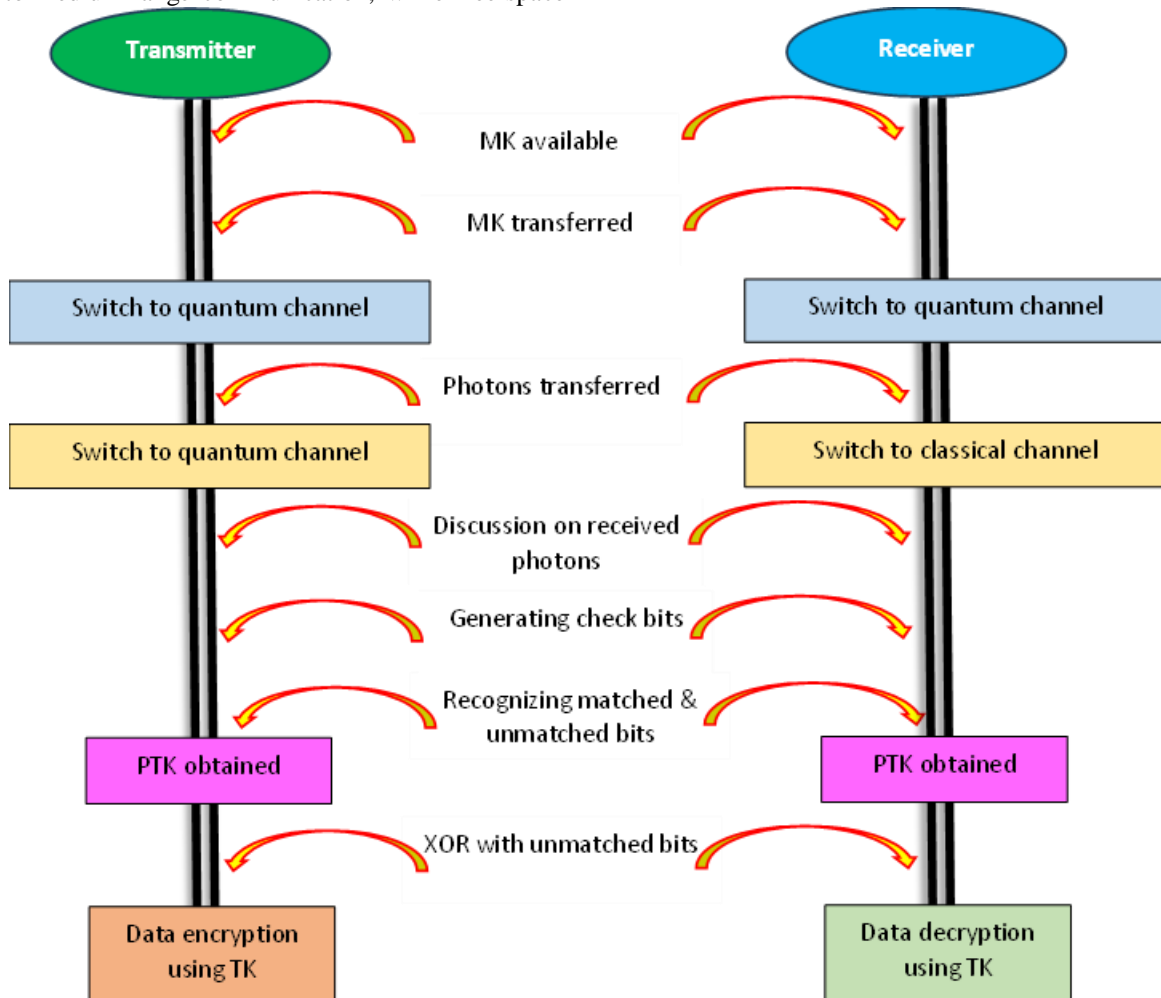


Figure 13 Key Generation and Communication Establishment in EBB92 Protocol

The network consists of Zigbee routers grouped as 'C_n' clusters among 'n' number of WBAN nodes.

1. Initially the available Master key (MK) is transferred between both the receiving party and transmitting party.
2. The process is then switched to the quantum channel, where the photons are transmitted via the free space to the receiver (Bob)
3. Once the photon transmission is stopped, the process switches over to the classical channel, where a two-way communication occurs between both the parties.
4. Now, the matched bits are identified and the necessary error estimation and corrections are done along with privacy amplification.

5. The matched bits form the quantum temporal key and the transmitting party XORs the matched bits with the unmatchable bits to form the last secret key, with which the encryption of the data is done.

Photon detector and polarization analyzer are equipped with both the transmitter and the receiver. The analyser is randomly adjusted by the receiver to one of the two directions orthogonal to the direction of the sender whenever photon is sent by the transmitter shown in Figure 13. This portion describes the Key generation process using the QuV is simulator. Sometimes the bits that are broadcast are either "0" or "1" because the receiver determines that the polarization is certain. For example, the bit results in the receiver receiving a photon while the analyser is set to 90°. The state cannot be predicted, if no photon is detected. To create the key, the sender and recipient both monitor the bits that are observed in

RESEARCH ARTICLE

this order. Let's take an example where both parties show signs of random polarization. The amounts of bits and polarizer that are sent and received are shown in Table 2.

Table 2 Key Generation Process During Communication

Bits	Transmitter		Receiver		Key	
	Polarisation angle	Bit Sent	Polarisation angle	Bit Detected		
1	+46	1	92	Yes(1)	1	
2	0	0	-46	No		
3	+46	1	-46	No		
4	0	0	-46	No		
5	+46	1	92	No	1	
6	+46	1	92	No		
7	0	0	92	No		
8	+46	1	92	Yes(1)		
9	0	0	-46	Yes(0)		0
10	+46	1	90	No		

The rate at which shared secret keys are generated between nodes is a critical performance metric in QKD. Key generation rates depend on various factors including the efficiency of the QKD protocol, transmission distance, and characteristics of the quantum channel. Efficient key generation rates are essential for establishing secure communication channels between sensor nodes in WBSNs. While QKD provides unconditional security for key distribution, it is often integrated with classical cryptographic techniques for practical applications. Symmetric encryption algorithms such as Advanced Encryption Standard (AES) are commonly used to encrypt data transmitted over classical channels, providing an additional layer of security. Classical error correction and privacy amplification algorithms are also integrated to correct errors in the generated keys and enhance their randomness, further strengthening the security of the communication channel. By incorporating QKD into the Hybrid Improved Unequal Secure Cluster-based Distributed Routing Protocol, the security of communication channels in WBSNs is significantly enhanced, ensuring the confidentiality and integrity of sensor data transmitted over the network. Moreover, leveraging QKD enables efficient key generation, error management, and classical integration, contributing to the overall performance improvement of the WBSN.

3.8. Energy Efficient Communication Protocols

Energy-efficient communication protocols are pivotal in extending the lifespan and optimizing the performance of Wireless Body Sensor Networks (WBSNs). One prominent protocol, Low-Energy Adaptive Clustering Hierarchy (LEACH), organizes nodes into clusters where each cluster elects a cluster head (CH). The CH aggregates data from its cluster members and transmits it to the base station, reducing the need for all nodes to send data directly over long distances. To balance energy consumption, the role of the CH rotates periodically, ensuring that no single node is

overburdened and depletes its energy prematurely. Another effective protocol is Power-Efficient Gathering in Sensor Information Systems (PEGASIS), which forms chains of nodes so that each node communicates only with its closest neighbor. This chain structure significantly reduces the number of transmissions and the distances over which data must travel. A designated node in the chain is responsible for sending the aggregated data to the base station, further conserving energy by minimizing the need for long-range communications.

Threshold Sensitive Energy Efficient Network (TEEN) is tailored for time-critical applications, where nodes transmit data only when sensor readings exceed certain predefined thresholds. This protocol reduces unnecessary data transmissions by ensuring that only significant data, which meets the threshold criteria, is sent. This not only saves energy but also reduces data congestion, making the network more efficient. These energy-efficient communication protocols, by strategically managing data transmission and leveraging hierarchical structures, play a crucial role in maintaining robust and energy-efficient operations in WBSNs.

3.9. Hardware Design Strategies for Energy-Efficient Wireless Body Sensor Networks (WBSNs)

Designing energy-efficient hardware for Wireless Body Sensor Networks (WBSNs) involves several key strategies aimed at minimizing power consumption while ensuring reliable performance. One critical approach is the selection of low-power microcontrollers, such as the ARM Cortex-M series or MSP430, which are optimized for low energy consumption. These microcontrollers should be programmed to utilize various sleep modes, activating only when necessary to process data or communicate, thereby conserving energy. In addition to efficient microcontrollers, implementing duty

RESEARCH ARTICLE

cycling for sensors significantly reduces power usage. Sensors can be periodically turned on and off, only collecting data when required, which helps to extend battery life.

Integrating energy-harvesting technologies, such as solar cells or kinetic energy harvesters, can provide supplementary power sources, reducing the dependence on batteries and prolonging operational periods. Another crucial aspect is the use of efficient communication protocols, which minimize energy spent on data transmission by aggregating data at intermediate nodes or using short-range communications before relaying data to a central node. Hardware components should be chosen based on their energy profiles, ensuring that every component, from sensors to communication modules, contributes to overall energy efficiency. By combining these hardware design strategies, WBSNs can achieve prolonged battery life, reliable performance, and efficient operation, essential for continuous health monitoring applications.

3.10. Case Study 1: Healthcare Monitoring System

Imagine a healthcare monitoring system deployed in a hospital environment where WBSNs are used to continuously monitor patients' vital signs such as heart rate, blood pressure, and temperature. The IUSCDRP-QKD protocol ensures secure and reliable communication between sensor nodes, protecting sensitive patient data from unauthorized access or tampering.

3.10.1. Scenario

- **Use Case:** A patient is admitted to the intensive care unit (ICU) with a critical medical condition requiring continuous monitoring.
- **Implementation:** WBSNs equipped with sensors are attached to the patient's body to monitor vital signs in real-time.
- **Protocol Integration:** The IUSCDRP-QKD protocol is implemented to establish secure communication channels between sensor nodes, ensuring confidentiality and integrity of patient data.
- **Simulation:** Simulations are conducted to evaluate the performance of the protocol in terms of key generation rates, error rates, and communication latency in a healthcare environment.

3.11. Case Study 2: Environmental Monitoring Network

Consider an environmental monitoring network deployed in a remote area to monitor air quality, temperature, and humidity levels. WBSNs equipped with sensors collect data and transmit it to a central monitoring station for analysis. The IUSCDRP-QKD protocol secures communication channels, protecting environmental data from unauthorized access or manipulation.

3.11.1. Scenario

- **Use Case:** An environmental monitoring network is deployed in a forest reserve to monitor air quality and detect potential pollution sources.
- **Implementation:** WBSNs consisting of sensor nodes are deployed at various locations within the forest reserve to collect environmental data.
- **Protocol Integration:** The IUSCDRP-QKD protocol is integrated into the network to establish secure communication channels between sensor nodes and the central monitoring station.
- **Simulation:** Simulations are conducted to assess the performance of the protocol under various environmental conditions, such as heavy rainfall or dense vegetation, to ensure reliable communication.

3.12. Case Study 3: Industrial IoT System

In an industrial Internet of Things (IoT) system, WBSNs are deployed in industrial settings to monitor equipment performance, detect faults, and optimize production processes. The IUSCDRP-QKD protocol ensures secure communication between sensor nodes, safeguarding critical operational data from cyber threats and unauthorized access.

3.12.1. Scenario

- **Use Case:** An industrial IoT system is deployed in a manufacturing plant to monitor equipment health and optimize production efficiency.
- **Implementation:** WBSNs equipped with sensors are installed on machinery and production lines to collect real-time data on performance metrics.
- **Protocol Integration:** The IUSCDRP-QKD protocol is integrated into the network architecture to establish secure communication channels between sensor nodes and the central control system.
- **Simulation:** Simulations are conducted to evaluate the performance and scalability of the protocol in a dynamic industrial environment with high data traffic and stringent security requirements.

4. RESULTS AND DISCUSSIONS

NS2 is needed when the simulation application. The outcomes of the IUSCDRP-QKD under a number of factors are validated by this section. At first, the functions of unequal clustering are confirmed using the system lifetime and effort effectiveness. For easiness, a great MAC level and error free correspondence contacts are grabbed. Next, each node's energy consumption is calculated along with a relative examination is additionally performed. And, first order stereo

RESEARCH ARTICLE

energy design is utilized for creating a model and also the variables are revealed. For evaluating the outcomes of the given IUSCDRP-QKD dependability in addition to energy effectiveness, a number of tests have been carried through of terminology of throughput, typical recurring energy more than a number of rounds and community lifetime of regards to variety of in existence nodes. The throughput suggests the entire amount of packets effectively obtained in the spot on the complete quantity of packets transmitted within the system. Furthermore, the common recurring energy signifies the entire quantity of energy, on typical, is now contained in the system. Likewise, the variety of still living nodes belongs to the node matter, and that doesn't totally deplete the energy of it is within the system.

The IUSCDRP-QKD is split into 2 phases: irregular clustering and secure information transmission. The IUSCDRP-QKD supporters for dependability and top-notch energy effectiveness and then lengthy daily life. Its own clustering mechanism also is provided to get rid of orphan nodes, in addition to a cluster managing intend to lengthen the system lifetime. IUSCDRP-QKD is a hands-on process means that many of the routes are estimated right before these are necessary. When sensor nodes are fixed, a table-driven process (proactive process) is desirable to a reactive process (reactive process). Stochastic gradient descent is a widely recognized also popular method in a lot of Machine Learning algorithms, and also, it is the basis of Neural Networks. At first, each and every node includes a distinctive ID, a certification (issued by an expert, like the starting station), a distinctive shared crucial (shared together with the base station), so the base station's public element.

Table 3 Parameter Settings

Parameter	Value
Node Count	200
Area	100m x 100m
Location of Base Station	50m, 50m sensing field of center
Begin Energy	4J
ϵ_{mp}	0.0014 pJ/bit/m ²
Eelec	48 nJ/bit
ϵ_{fs}	10 pJ/bit/m ²
E_{DA}	5 nJ/bit/signal
Size of Packet	4000 bits

The certification is utilized to authenticate some node together with the starting station's public element during neighbour detection; a distinctive shared key element is utilized to come in contact with the base station throughout the network's lifetime. The parameter settings shown in Table 3.

Figure 14 displays the comparability of Sec-LEACH and IUSCDRP-QKD of terminology of throughput under an altering variety of assailants. By this particular figure, it is obvious that all through is rather high plus it is likely to somewhat reduce with an increased variety of assailants. When it comes to the bare minimum of two assailants, an optimum throughput of just 80.5 is required. Ultimately, an optimum throughput of 81.5 is achieved within the existence of one assailant. These result values indicate the degraded functionality with all the existence of addition of proposed approach. Ultimately, it could be concluded the IUSCDRP-QKD attained optimum throughput when compared with SEC-LEACH.

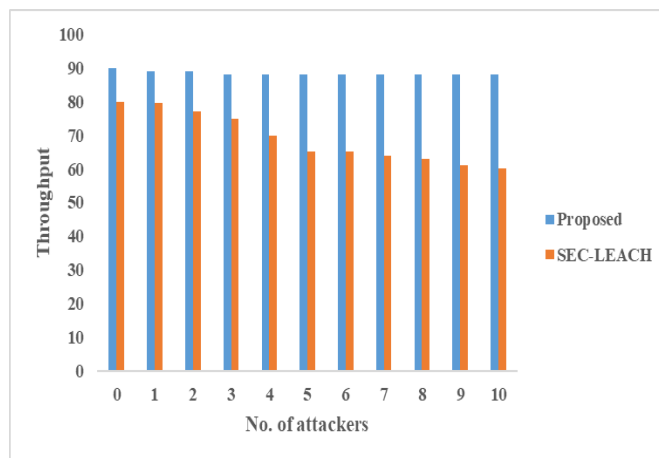


Figure 14 No. of Attackers Versus Throughput

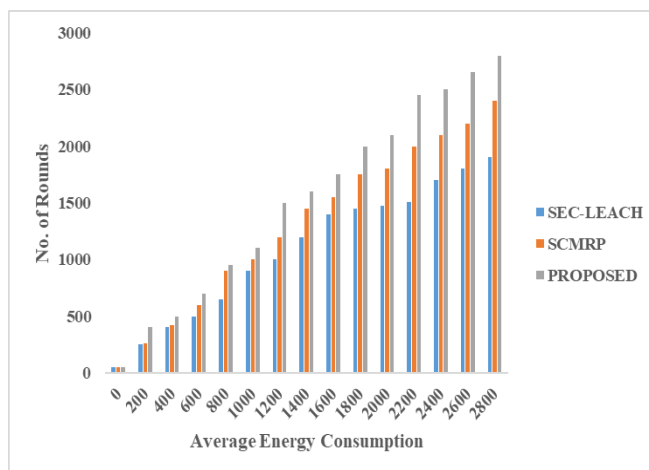


Figure 15 Energy Efficiency Analysis

RESEARCH ARTICLE

Figure 15 displays the energy effectiveness evaluation on the IUSCDRP-QKD process with all the current SEC-LEACH and SCMRP process of conditions of typical recurring energy. Figure 16 analyses the outcomes gotten by different techniques within terminology of community lifetime. Because there are varied techniques utilized to evaluate the lifespan of WSN, the variety of still living nodes is recognized as in this case. By the Figure 16, it is understood that the provided IUSCDRP-QKD stretches the system lifespan and also stretches the demise of the nodes within WSN.

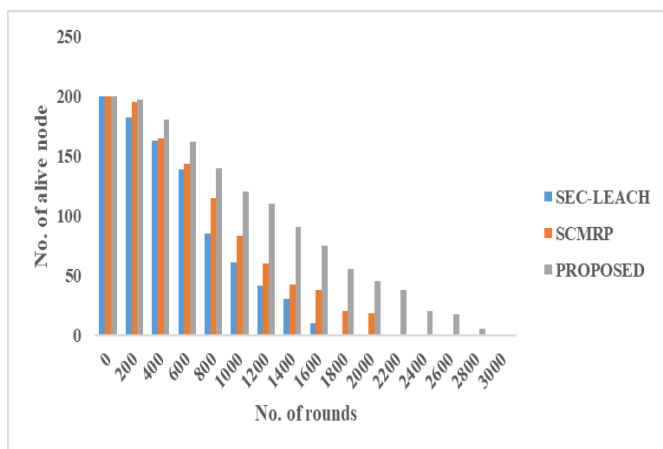


Figure 16 Network Lifetime Analysis

Table 4 Comparing the Network Lifetime Analysis with Different Models

Method	HND	LND	FND
SEC-LEACH	942	1905	91
SCMRP	1073	2352	189
PROPOSED	1412	3173	317

Table 4 and Figure 17 present the network lifetime evaluation of terminology of FND, LND and HND of the proposed and pre-existing techniques. It is apparent the provided method slowed the demise of very first node rounds in comparison with various other techniques. As the number of quantum bits rises, the key generation time also gradually increases shown in Figure 18.

Intruders are constantly ready to obtain the network key and use it to access data from networks. However, networks are susceptible to quantum assaults including beam splitting, time-shift, and intercept/resend. In such case, the fact that the receiver picked up a photon suggests that the unblinded detector is the sole one with that capability. Consequently, the Eavesdropper understands the importance of this piece significance of bits.

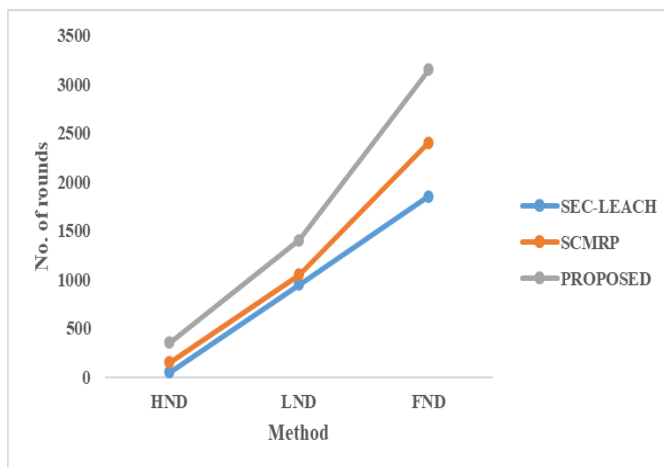


Figure 17 Comparing the Network Lifetime Analysis with Different Models

Note: FND – First Node Expires; LND – Previous Node Dies; HND – Node Dies

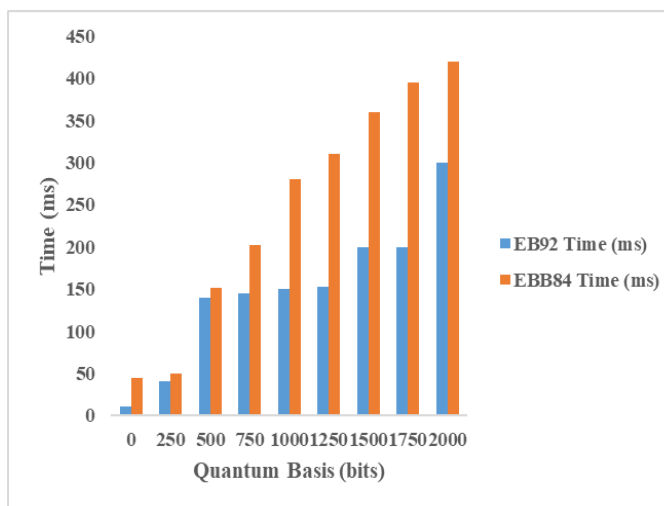


Figure 18 Time Complexity Analysis of EB92 and EBB84 Protocols

Table 5 Energy Usage Comparison of Proposed and Existing Systems

Protocol	Energy Usage
IUSCDRP-QKD	Low
SCMRP	Medium
SEC-LEACH	High

RESEARCH ARTICLE

This comparison is based on theoretical assessments and simulations, considering factors such as energy consumption during key generation, routing overhead, and data transmission. The IUSCDRP-QKD protocol is expected to exhibit lower energy usage compared to SCMRP and SEC-LEACH due to its efficient routing algorithm and secure communication mechanism facilitated by QKD shown in Table 5. The exact energy usage may vary depending on specific network configurations, environmental conditions, and implementation details. Conducting detailed simulations and experiments would provide more accurate insights into the energy efficiency of each protocol.

Table 6 Comparison of Increasing Number of Nodes vs. Latency of Proposed and Existing Systems

Number of Nodes	IUSCDRP-QKD Latency	SCMRP Latency	SEC-LEACH Latency
50	Low	Medium	High
100	Low - Medium	Medium-High	High
200	Medium	High	Very High

This comparison is based on theoretical assessments and simulations, considering factors such as routing overhead, packet transmission delay, and network congestion shown in Table 6. The latency performance of each protocol may vary depending on the network topology, traffic patterns, and processing capabilities of the nodes. IUSCDRP-QKD protocol is expected to exhibit lower latency compared to SCMRP and SEC-LEACH due to its efficient routing algorithm and secure communication mechanism facilitated by QKD.

Table 7 Comparison of Increasing Number of Nodes vs. Overhead of Proposed and Existing Systems

Number of Nodes	IUSCDRP-QKD overhead	SCMRP overhead	SEC-LEACH overhead
50	Low	Medium	High
100	Low - Medium	Medium-High	High
200	Medium	High	Very High

This comparison considers factors such as routing overhead, key distribution overhead (in the case of IUSCDRP-QKD), and additional computational costs incurred by each protocol as the network scales. While IUSCDRP-QKD is expected to exhibit relatively lower overhead due to its efficient routing algorithm and secure communication mechanism facilitated

by QKD, SCMRP and SEC-LEACH may experience higher overhead as the number of nodes increases shown in Table 7. The exact overhead performance may vary depending on network configurations, traffic patterns, and implementation details. Conducting detailed simulations and experiments would provide more accurate insights into the overhead characteristics of each protocol.

5. CONCLUSION

This is due to the dependence of the mechanism to the uncertainty principle meaning, the instances cannot be predicted by the intruders under any circumstances. The complex structure of the method put-forth with respect to time and the comparative analysis of the protocol effectiveness is done and represented. The method put-forth will result in less time complexity for Key generation as compared with that of the EBB84 protocol and secure the network against Time shift quantum attack. The intent of furtherance of this work's direction is to increase the percentage of efficiency of the protocol. To attain energy-efficient and reliable details transmission of WSN, with this paper, created a secured unequal clustering process known as IUSCDRP-QKD community lifetime. The considerable simulation demonstrated the provided IUSCDRP-QKD given the demise on the sensor node; then enhanced the throughput underneath the existence of assailants. As a portion long term tasks, the offered IUSCDRP-QKD strategy has the ability to incorporate hybrid car algorithms for uneven WSN clustering.

REFERENCES

- [1] Iqbal, S., Ahmed, A., Siraj, M., Al Tamimi, M., Bhangwar, A. R., & Kumar, P. (2023). A Multi-hop QoS-aware and Predicting Link Quality Estimation (PLQE) Routing Protocol for Reliable WBSN. *IEEE Access*.
- [2] Jayabalan, E., & Pugazendi, R. (2023). An efficient routing protocol for wireless body sensor networks using reinforced learning algorithm in clusters. *Measurement: Sensors*, 27, 100730.
- [3] Kalaivani, V. (2023). Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications. *Personal and ubiquitous computing*, 27(3), 875.
- [4] Nassra, I., & Capella, J. V. (2023). Data Compression Techniques in IoT-enabled Wireless Body Sensor Networks: A Systematic Literature Review and Research Trends for QoS Improvement. *Internet of Things*, 100806.
- [5] Kumar, C. R., Kumar, T. G., Hemlathadhevi, A., & Thirupurasundari, D. R. (2023). An Energy Efficiency Based Secure Data Transmission in WBSN Using Novel Id-Based Group Signature Model and SECC Technique. *Journal of Internet Technology*, 24(3), 683-696.
- [6] Ramalingam, V., Saminathan, R., & Baalamurugan, K. M. (2023). SDT-ORFC: Securing data transmission using on route cluster frequency Propagation based on segregate neighbor fragmentation path routing in WBSN.
- [7] Parthiban, L., Latchoumi, T.P., Balamurugan, K., Raja, K. and Parthiban, R., 2023. Cognitive Computing for the Internet of Medical Things. In *Integrating Blockchain and Artificial Intelligence for Industry 4.0 Innovations* (pp. 85-100). Cham: Springer International Publishing.
- [8] Lu, Z., Zhao, Y., Li, X., & Xu, C. Z. (2023). Randomized Passive Energy Beamforming for Cooperative Localization in Reconfigurable

RESEARCH ARTICLE




- Intelligent Surface Assisted Wireless Backscattered Sensor Network. *IEEE Internet of Things Journal*.
- [9] Singh, P., Raw, R. S., & Le, D. N. (2023). A Framework for Hybrid WBSN-VANET-based Health Monitoring Systems. In *Computational Intelligent Security in Wireless Communications* (pp. 51-62). CRC Press.
- [10] Ramalingam, V., Saminathan, R., & Baalamurugan, K. M. (2023). Fork-Hook encryption policy based secured Data Centric Routing Gateway for proactive trust ware data transmission in WBSN. *Measurement: Sensors*, 27, 100760.
- [11] Angelucci, A., Camuncoi, F., Dotti, F., Bertozzi, F., Galli, M., Tarabini, M., & Aliverti, A. (2023, September). A Wireless Body Sensor Network for Cardiorespiratory Monitoring During Cycling. In *2023 IEEE International Workshop on Sport, Technology and Research (STAR)* (pp. 1-4). IEEE.
- [12] Balamurugan, K., Latchoumi, T.P., Deepthi, T. and Ramakrishna, M., 2023. Optimization Studies on Al/LaPO₄ Composite Using Grey Relational Analysis. In *Metal Matrix Composites* (pp. 29-48). CRC Press.
- [13] Iqbal, S., Bhangwar, A. R., Ahmed, A., Ahmed, F., Awais, M., & Hussain, A. (2023). RLTD: A Reliable, Link Quality, Temperature and Delay Aware Routing Protocol for Wireless Body Sensor Networks.
- [14] Akilan, S. S., & Sekar, J. R. (2023). OTP-Q encryption and Diffie-Hellman mutual authentication for e-healthcare data based on lightweight S-WBSN framework. *Technology and Health Care*, (Preprint), 1-18.
- [15] Yakubu, A. A., Shuaibu, S., & Adamu, A. T. (2023). Wireless Body Sensor Network Applied to Blood Pressure Monitoring System. *African Journal of Advances in Science and Technology Research*, 11(1), 53-62.
- [16] Surla, G., & Lakshmi, R. (2023). Design and evaluation of novel hybrid quantum resistant cryptographic system for enhancing security in wireless body sensor networks. *Optical and Quantum Electronics*, 55(14), 1252.
- [17] Mishra, I., Jain, S., & Maik, V. (2023). Secured ECG Signal Transmission Using Optimized EGC with Chaotic Neural Network in WBSN. *Comput. Syst. Sci. Eng.*, 44, 1109-1123.
- [18] Sandhya, M., & Anjaneyulu, L. (2023). Compact, flexible triple band Sierpinski fractal antenna on a Hilbert patterned ground for W-WBSN. *Microwave and Optical Technology Letters*.
- [19] Alatawi, M. N. A Hybrid Cryptography and LogiXGBoost Model for Intelligent and Privacy Protection in Wireless Body Sensor Networks (WBSNS).
- [20] Petrenko, A. (2023, September). Approaches for WSN (Wireless Sensor Networks) Standardization and Their Interoperability in Combining into a Global Network. In *2023 IEEE East-West Design & Test Symposium (EWDTS)* (pp. 1-4). IEEE.
- [21] Jain, R. (2023, July). A Time-Sensitive Protocol for Wireless Sensor Networks' Communication. In *2023 International Conference on Data Science and Network Security (ICDSNS)* (pp. 01-07). IEEE.
- [22] Din, R. U., Bangash, J. I., Ullah, Z., Khan, A. W., Ullah, H., & Khan, F. U. Temperature Aware and Energy-Efficient Routing for Wireless Body Area Network.
- [23] Latchoumi, T.P., Swathi, R., Vidyasri, P. and Balamurugan, K., 2022, March. Develop new algorithm to improve safety on WMSN in health disease monitoring. In *2022 International Mobile and Embedded Technology Conference (MECON)* (pp. 357-362). IEEE.
- [24] Balamurugan, K., Latchoumi, T.P. and Ezhilarasi, T.P., 2022. Wearables to improve efficiency, productivity, and safety of operations. In *Smart Manufacturing Technologies for Industry 4.0* (pp. 75-90). CRC Press.
- [25] Kumar, S., Rathore, N. K., Prajapati, M., & Sharma, S. K. (2023). SF-GoER: an emergency information dissemination routing in flying Ad-hoc network to support healthcare monitoring. *Journal of Ambient Intelligence and Humanized Computing*, 14(7), 9343-9353.
- [26] Alhusein, D., & Idrees, A. K. (2023). A Comprehensive Review of Wireless Medical Biosensor Networks in Connected Healthcare Applications. *Enabling Technologies for Effective Planning and Management in Sustainable Smart Cities*, 229-244.
- [27] Zaman, K., Sun, Z., Hussain, A., Hussain, T., Ali, F., Shah, S. M., & Rahman, H. U. (2023). EEDLABA: Energy-Efficient Distance-and Link-Aware Body Area Routing Protocol Based on Clustering Mechanism for Wireless Body Sensor Network. *Applied Sciences*, 13(4), 2190.
- [28] Gaikwad, V. D., & Ananthakumaran, S. (2023). A Review: Security and Privacy for Health Care Application in Wireless Body Area Networks. *Wireless Personal Communications*, 130(1), 673-691.
- [29] Mavinkattimath, S., Khanai, R., Torse, D., & Iyer, N. (2023). HS-HA: Design of High-Speed Hardware Accelerator SOC for Biomedical Applications.
- [30] Mavinkattimath, S., Khanai, R., Torse, D., & Iyer, N. (2024). Design and implementation of low-power, high-speed, reliable and secured Hardware Accelerator using 28 nm technology for biomedical devices. *Biomedical Signal Processing and Control*, 88, 105554.
- [31] Hosseinzadeh, M., Mohammed, A. H., Rahmani, A. M., A. Alenizi, F., Zandavi, S. M., Yousefpoor, E., ... & Tighiz, L. (2023). A secure routing approach based on league championship algorithm for wireless body sensor networks in healthcare. *Plos one*, 18(10), e0290119.
- [32] Chitra, S., Kannan, S., & Sundar Raj, A. (2023). Improvement of life time for wireless body sensor networks using optimal clustering and routing protocol. *Journal of Intelligent & Fuzzy Systems*, 44(2), 1673-1690.
- [33] Matloob, T. (2023). On the Design of Efficient and Secure Heterogenous Generalized Signcryption for Wireless Body Sensor Networks (Doctoral dissertation, CAPITAL UNIVERSITY).
- [34] Saad, G., Harb, H., Abouaissa, A., Idoumghar, L., & Charara, N. (2023). A sensing-based patient classification framework for efficient patient-nurse scheduling. *Sustainable Computing: Informatics and Systems*, 38, 100855.
- [35] Latchoumi, T.P., Parthiban, L., Balamurugan, K., Raja, K., Vijayaraj, J. and Parthiban, R., 2023. A Framework for Low Energy Application Devices Using Blockchain-Enabled IoT in WSNs. In *Integrating Blockchain and Artificial Intelligence for Industry 4.0 Innovations* (pp. 121-132). Cham: Springer International Publishing.
- [36] Pugazhendhi, L.T., Kothandaraman, R. and Karnan, B., 2022. Implementation of visual clustering strategy in self-organizing map for wear studies samples printed using FDM. *Traitement du Signal*, 39(2), p.531.
- [37] Abdelnaeim, N. T., Fahmy, H. M., & Hady, A. A. (2023). DC-PHD: multitarget counting and tracking using binary proximity sensors. *International Journal of Wireless and Mobile Computing*, 25(4), 328-339.
- [38] Wasay Mudasser, A., & Ahmed Abdul Gafoor, S. A. (2023). Secure Internet of Things based hybrid optimization techniques for optimal centroid routing protocol in wireless sensor network. *Concurrency and Computation: Practice and Experience*, 35(6), 1-1.
- [39] Cao, T. (2023). Analysis of aerobic training posture using machine vision for body area networks. *Wireless Networks*, 29(4), 1611-1620.
- [40] Verma, H., Chauhan, N., & Awasthi, L. K. (2023). A Comprehensive review of 'Internet of Healthcare Things': Networking aspects, technologies, services, applications, challenges, and security concerns. *Computer Science Review*, 50, 100591.
- [41] Shyja, V. I., Ranganathan, G., & Bindhu, V. (2023). Link quality and energy efficient optimal simplified cluster-based routing scheme to enhance lifetime for wireless body area networks. *Nano Communication Networks*, 100465.
- [42] Le Moullec, Y., Uguen, P. B., Mercier, I. E., DIGUET, D. J. P., & SENTIEYS, P. O. Architecture of Ultra Low Power Node for Body Area Network.
- [43] Selvi, G. V., Rathna, N., Lizy, R., Prabavathy, S., & Aurchana, P. (2023, September). Energy aware clustering for biomedical wireless sensor networks. In *AIP Conference Proceedings* (Vol. 2831, No. 1). AIP Publishing.

RESEARCH ARTICLE




- [44] Kumar, R., Agarwal, P., Panda, S., & Gupta, S. K. (2023, June). A study on IoT-based smart hospital system. In AIP Conference Proceedings (Vol. 2782, No. 1). AIP Publishing.

Authors






Dr Prakash Muthusamy    is currently working as Assistant professor in the Department of Information Technology, Sri Krishna Adithya College of Arts and Science, Coimbatore. He received his doctoral degree from Bharathiar University, Coimbatore. He has 5 years of teaching experience. He has published one Patent and research papers in various National, International Journals and authored one book. Also, he acted as a resource person in seminars and workshops. He received two awards for academic excellence. He is acting as editorial member in peer reviewed journals.



Dr Senthil Kumar S    received his first degree from Madras University, Computer Science, India, in 2005. He has also Master degree from Thiruvalluvar University, Computer Applications, India, in 2008. The Ph.D. degree from the Department of Computer Applications in Manonmaniam Sundaranar University, India in 2019. He is currently serving as an Assistant Professor in Department of Computer Applications at SRM Institute of Science and Technology, Tiruchirappalli, Tamil Nadu, India. His main




research interests focus on Web Metrics, Web Services, Computer Networks, Image Processing, Data Mining, and Text Mining.



Dr Kanagalakshmi K    is working as an Associate Professor in the Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology (Deemed to be University), Trichy, Tamilnadu, India. She has 23 years of teaching experience the collegiate education. She has published more than 34 research papers in International Journals of repute and presented more than 75 papers in International, National and State level Seminars, Conferences together. She has

produced M.Phil. and Ph.D. Scholars. She has published 5 books and 3 Patents. She has received 8 awards like Best Faculty Award, Best Scientist Award, Best Principal Award etc. Her areas of interest include Biometric, Pattern Recognition, Digital Image Processing, Security etc.



Dr Sreejith Vignesh B P    is currently working as Associate professor and Head of the Department of Information Technology, Sri Krishna Adithya College of Arts and Science, Coimbatore. He has 13 years of Experience in teaching and research. He has been awarded the Doctoral degree by Bharathiar University in the year 2019. He has completed his B. Sc Computer Technology and M.Sc. Software Engineering from Kongu Engineering College and completed his MBA in Human Resource Management and MCA from Bharathiar University. He has been conferred with the Degree of Doctor of Philosophy from the esteemed Bharathiar University, Coimbatore. In addition to this he is a Cisco Certified Network Associate and also grabs Oracle Certifications from Oracle Gym. He is a member of Various renowned Professional Bodies like ISTE, IACSIT, ISRD, IAAPC, IAE etc. He is a NASSCOM Certified Life Skill Trainer and Fraghren Academy Certified Soft Skill Trainer, He Is a Microsoft Certified Innovative Educator and Google Certified Digital Marketer.

How to cite this article:

Prakash Muthusamy, Senthil Kumar S, Kanagalakshmi K, Sreejith Vignesh B P, “ A Hybrid Improved Unequal Secure Cluster Based Distributed Routing Protocol with Quantum Key Distribution to Improve the Performance Measures in Wireless Body Sensor Network ”, International Journal of Computer Networks and Applications (IJCNA), 11(4), PP: 407-427, 2024, DOI: 10.22247/ijcna/2024/26.